Af

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Applicants: MOLDOVYAN et al.   Attorney Docket: P65855US0

Serial No.:   09/622,047   Group Art Unit: 2132

Filing Date: August 23, 2000   Examiner: Benjamin E. LANIER

For: METHOD FOR THE BLOCK-ENCRYPTION OF DISCRETE DATA

TRANSMITTAL

MAIL STOP REPLY BRIEF - PATENTS
Commissioner for Patents
P.O. Box 1450
Alexandria, VA   22313-1450

Sir:

In response to the Examiner's Answer mailed August 17, 2007, transmitted herewith is Applicants' REPLY BRIEF under 37 CFR 41.41.
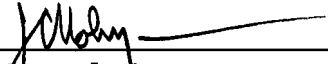
The fee has been calculated as shown below:

Claims Remaining After Amendment	Highest Number Previously Paid For	Present Extra	Small Entity		Other Than A Small Entity	
			Rate Addit. Fee	(or)	Rate Addit. Fee	
Total 3	- 20	= 0	x25 = $		x 50 = $	
Indep. 1	- 3	= 0	x105 = $		x 210 = $	
Total Additional Fee			$		$	

XX   If a Petition for Extension of Time is necessary and the Petition and/or the check is not enclosed, this will act as the Petition and applicant herewith petitions the Commissioner to extend the time for response and charge any fees necessary under 37 CFR 1.17 (a)(1)-(5) to Deposit Account No. 06-1358. The Commissioner is also authorized to charge payment of any other additional fees associated with this communication or credit any overpayment to Deposit Account No. 06-1358. A duplicate copy of this sheet is attached.

JACOBSON HOLMAN, PLLC

Dated: October 17, 2007   By:_____
400 Seventh Street, N.W.   John C. Holman
Washington, D.C.   20004-2201   Reg. No. 22,769
(202)638-6666
JCH/JC

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

In re Application of:	Confirmation Number: 4150
MOLDOVYAN et al.	Attorney Docket: P65855US0
Serial No. 09/622,047	Group Art Unit: 2132
Filed: August 23, 2000	Examiner: Benjamin E. LANIER

For: METHOD FOR THE BLOCK-ENCRYPTION OF DISCRETE DATA

<u>**REPLY BRIEF UNDER 37 C.F.R. §41.41**</u>

MAIL STOP APPEAL BRIEF - PATENTS
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

    This is a reply brief in response to the Examiner's Answer mailed August 17, 2007 regarding the above-referenced application.

    Status of claims begins on page 2 of this paper.

    Grounds of rejection to be reviewed on appeal appear on page 3 of this paper.

    Argument begins on page 4 of this paper.

I. **STATUS OF THE CLAIMS**

The appealed claims are Claims 1, 3, and 5, which are currently pending in this application. Claims 1, 3, and 5 stand rejected under 35 U.S.C. § 102 (b) as allegedly being anticipated by Schneier (Bruce Schneier, Applied Cryptography, 1996, John Wiley & Sons, copies were previously enclosed in the Evidence Appendix of the Appeal Brief). A copy of the claims on appeal appears in the attached Claims Appendix.

II. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Whether Claims 1, 3, and 5 are properly rejected under 35 U.S.C. § 102 (b) as being anticipated by Schneier (Bruce Schneier, Applied Cryptography, 1996, John Wiley & Sons).

III. **ARGUMENT**

Claims 1, 3, and 5 Are Not Anticipated by Schneier Reference Because It Does Not Teach
or Suggest All the Limitations of These Claims

The Examiner's Answer of August 17, 2007 has been carefully considered. However, Applicant respectfully submits that, Schneier does not disclose any feature of the present invention as defined in Claims 1, 3 and 5. Thus, the final rejections of the application are based on 35 U.S.C. 102 (b) is incorrect and should be withdrawn.

More specifically, the Examiner asserts that the book of Schneier, in the "The P-Box Permutation" section (page 275), describes the data-dependent permutation operation **P**. The Examiner calls this operation a direct permutation (in accordance with the Schneier term).

Applicant, in the Appeal Brief as well as in previous amendments, denoted this operation as **P**(Z) and respectfully submits that based on the description in the book of Schneier, this operation is a fixed permutation and is independent of the data. This is stated in the following extract from the Appeal Brief:

> In the Final Office Action, the Examiner indicated that Schneier discloses key bit permutation operation depending on the data being converted. The issue is how to correctly interpret the disclosure of Schneier by a person of ordinary skill in the art.

> Applicant respectfully submits that, Schneier, when describing algorithm DES (US Data Encryption Standard), does not disclose any feature of converting a subkey depending on data being converted. Fig.12.1 of Schneier shows a general diagram of data conversion in accordance with the encryption algorithm DES, which includes 16 rounds of conversion. In each round of conversion, based on a right subblock R and subkey K, function $f = f(R, K)$ is calculated, after which a left

4

subblock L is converted by performing on it the operation XOR: $L: = L \oplus f(R, K)$, where ": =" is the designation of assignment operation. Between the preceding and subsequent encryption rounds, the subblocks are transposed (swapped). Thus, it is important to ascertain, how conversion $f(R, K)$ is performed. In the Examiner's view, in calculating $f(R, K)$, the operation of permuting subkey bits **depending on data being converted** is used. However, Applicant's detailed study of Schneier has shown that this is not the case. More specifically, Schneier shows that the procedures of calculating the function $f(R, K)$ includes consecutive performing the following operations:

- operation of broadening L 32-bit data subblock to X broadened 48-bit data subblock;

- conversion of the broadened subblock by means of its addition with 48-bit subkey $X: = X \oplus K$ (before this step, no conversions depending on the data block being converted have been performed on this round subkey, i.e. **no permuting subkey bits depending on data has been performed**);

- performing a cascade of substitution operations of 6x4 size implementing the substitution operation S_{6x4}, as a result of which the broadened 48-bit subblock is converted into 32-bit binary vector $Z: Z = S_{6x4}(X)$;

- performing the transmutation operation P which consists in a fixed permutation of the vector Z bits, i.e. permutation of the vector Z bits is performed independently of the value of some data subblock but always in the same manner, as prescribed by the Schneier reference. After performing operation P, the value of $f(R, K)$ is obtained, i.e. we have $f(R, K) = P(Z)$.

It is evident from this extract from the Appeal Brief that $P(Z)$ permutation is a fixed one.

In fact, a person of ordinary skill in the art can hardly imagine that, based on the description in Schneier, the operation $P(Z)$ can be interpreted as a data-dependent operation since it in general does not depend on anything and is a fixed operation and in hardware

implementation is an intertwining of conductors, i.e. rigid connection by a conductor of each input bit with some fixed output bit. Applicant hereby provides additional analysis supporting that operation $P(Z)$ fixed bit permutation. Indeed, it follows from the Schneier, "The P-Box Permutation" (page 275), that a bit from the predetermined order at the input of permutation $P(Z)$ always fits in the predetermined order at the output of permutation $P(Z)$ which is specified by table 12.7 (page 277 of Schneier) and this does not depend either of data or on a key. Moreover, if a minor change is made in table 12.7 (page 277 in Schneier), it will not be DES algorithm any more. Table 12.7 (page 277 in Schneier) clearly indicates that a bit from first in put order transfers to 8th order at the output, which can be denoted as 1->9. Similarly rigidly this table (and precisely it describes permutation operation $P(Z)$ predetermines links between the remaining input and output orders: 2->17, 3->23, 4->31, 5->13, 6->28, 7->2, 8->18, 9->24, 10->16, 11->30, 12->6, 13->26, 14->20, 15->10, 16->1, 17->8, 18->14, 19->25, 20->3, 21->4, 22->29, 23->11, 24->19, 25->32, 26->12, 27->22, 28->7, 29->5, 30->27, 31->15, 32->21. Evidently, these links do not depend on the fact, what values input bits to be permuted have. Therefore, input bit are permuted in a fixed manner, regardless of their values, and hence independent of whether input bits are key bits, or data bits, or binary vector bits being a result of joint conversion of a data subblock and round key. Any person skilled in this art would understand the description of permutation $P(Z)$ provided in the "P-Box Permutation" section (page 273) of Schneier in this way, i.e. he/she would inevitably recognize that operation $P(Z)$ in algorithm DES is a fixed permutation operation which is not a permutation operation that depends on data being converted.
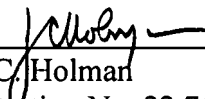
Thus, the conclusion in the Appeal Brief is quite correct to state: "[T]he above detailed operations have revealed that, in forming the value of $f(R, K)$ in the DES algorithm, **the operation of permuting subkey bits depending on data being converted is not used**. The vector Z bit transmuting operation performed in the cited method of block encryption (algorithm DES) is fixed and is performed **regardless of data being converted**. Schneier confirms this by describing the operation P in the section "The P-box permutation".

Therefore, the currently presented claims are not anticipated by Schneier and the rejection under 35 U.S.C. § 102 (b) has been overcome. Accordingly, withdrawal of the rejection under 35 U.S.C. § 102 (b) is respectfully requested.

Respectfully submitted,

JACOBSON HOLMAN PLLC

Date: October 17, 2007
(202) 638-6666
400 Seventh Street, N.W.
Washington, D.C. 20004

By_____
John C. Holman
Registration No. 22,769

Enclosed:

CLAIM APPENDIX

IV.   CLAIM APPENDEX

Claim 1 (previously presented):   A method for block encryption of discrete data, comprising the steps of: generating an encryption key in the form of a set of subkeys, breaking down a data block into $N \geq 2$ data subblocks and alternately converting said data subblocks by performing a two-place operation on the data subblock and the subkey, wherein, prior to carrying out said two-place operation on an i-th data subblock and a subkey, an operation of permuting subkey bits is performed on the subkey depending on the value of a j-th data subblock, where $i \neq j$.

Claim 2 (cancelled)

Claim 3 (previously presented):   The method according to claim 1, wherein an operation of cyclic offsetting subkey bits depending on the value of the j-th data subblock is used as the j-th data subblock-dependent operation of permuting subkey bits.

Claim 4 (cancelled)

Claim 5 (previously presented)   The method according to claim 1, wherein the operation of permuting subkey bits is performed on one of said set of subkeys depending on the value of the j-th data subblock, where $i \neq j$, and the value of another subkey.